Serviciu de validare a semnăturilor digitale în conformitate cu standardele ETSI

- referat – stagiu practică I

coordonator-științific: Mihai-Lică PURA

autor: Ștefan BODOARCĂ

Cuprins

Introducere

Activitățile bancare, comercializarea, vânzarea și cumpărarea de bunuri sunt, în mod vizibil și de un timp îndelungat, dependente de tranzacțiile electronice, pentru ca toate aceste operațiuni să se desfășoare mai rapid și să ofere servicii îmbunătățite. Aceasta a dus la creșterea numărului de documente electronice generate, procesate, păstrate pe calculatoare și transmise prin rețea. Documentele electronice, asemenea celor în format fizic, conțin informație importantă și secretă care trebuie protejată de terțe părți rău intenționate (care nu sunt reprezentate nici de emițătorul și nici de receptorul informației) ce ar putea modifica această informație. Uneori, informația sau alte detalii relative la aceasta (data/timpul creării, trimiterii sau recepționării) trebuie protejate chiar împotriva intervenției emițătorului sau receptorului, deoarece și ei ar putea modifica un document în mod ilicit. [1]

În mod obișnuit, documentele în format fizic sunt validate și certificate de o semnătură scrisă ce are rolul de a asigura autenticitatea semnatarului. Pentru documentele electronice este necesar un mecanism asemănător. Semnăturile digitale, care nu sunt decât un șir de 0 și 1 generat folosind un algortim de semnătură digitală, au ca scop validarea și autentificarea documentelor electronice. Validarea se referă la procesul care certifică conținutul documentului, în timp ce autentificarea se referă la procesul de certificare a expeditorului documentului. [1]

Caracterisiticile semnăturilor scrise și ale semnăturilor digitale

O semnătură obișnuită trebuie să aibă următoarele caracteristici: stabilirea cu ușurință a autenticității semnăturii, dificultatea falsificării semnăturii, semnătura să nu poată fi transferată altei persoane, nonrepudierea astfel încât semnatarul să nu poată nega propria semnătură.[1]

O semnătură digitală trebuie să aibă toate caracteristicile amintite pentru o semnătură obișnuită, plus câteva caracteristici specifice, deoarece acest tip de semnare este folosit în mod practic în aplicații ce au caracter sensibil precum schimbul sigur de e-mail-uri, tranzacții bancare peste Internet, etc. Din moment ce o semnătură digitală este doar o secvență de 0 și 1, este de dorit ca aceasta să aibă următoarele proprietăți: semnătura să fie o înșiruire de biți care să depindă de mesajul semnat (astfel, semnătura va fi diferită pentru documente diferite, chiar dacă semnatarul este același); semnătura trebuie să folosească informație care este unică pentru semnatar pentru a preveni falsificarea și negarea semnării; trebuie să fie relativ ușor de produs; trebuie să fie relativ ușor de recunoscut, iar autenticitatea acesteia să fie ușor de verificat; din punct de vedere computațional, o semnătură digitală trebuie să fie imposibil de falsificat, ceea ce înseamnă că nu se poate construi un mesaj nou pentru o semnătura deja existentă sau că nu se poate construi o semnătură falsă pentru un anumit mesaj; trebuie ca semnăturile digitale să poată fi păstrate pe mecanisme de stocare pentru a rezolva posibile dispute mai târziu.[1]

Pentru a verifica autenticitatea emițătorului unui document și a faptului că acest document nu a fost modificat, au fost dezvoltate câteva proceduri, numite tehnici de autentificare. Totuși, tehnicile de autentificare a mesajelor nu pot fi folosite direct ca semnături digitale, deoarece tehnicile de autentificare au și anumite neajunsuri. Spre exemplu, cu toate că autentificarea mesajului protejează cele două părți implicate în schimbul de mesaje de o terță

parte, nu protejează cele două părți una de cealaltă. Mai mult, schemele elementare de autentificare produc semnături care au aceeași lungime ca mesajele în sine.[1]

Noțiuni de bază și de terminologie

Semnăturile digitale sunt compuse pe baza documentelor (mesaje/informație) care trebuie semnate și pe baza unor informații private, deținute numai de semnatar. În practică, în loc să se folosească tot mesajul, se aplică o funcție de hash pe mesaj pentru a se obține un rezumat al acestuia (eng. *message digest*). O funcție de hash, în acest context, primește la intrare un mesaj de lungime arbitrară și produce un rezumat al mesajului ce are o lungime fixă. Funcții de hash precum SHA-1, SHA-2, SHA-3 (SHA = *secure hash algorithm*) asigură faptul că este foarte puțin probabil pentru ca din două mesaje diferite să se obțină același hash. Există două largi tehnici folosite în formarea unei semnături digitale – criptosisteme cu chei simterice și criptosisteme cu chei publice (criptosistem, în sens larg, se referă la o tehnică de criptare). În criptosistemul cu chei simetrice este folosită o cheie secretă cunoscută doar de emițător și de receptorul legitim al mesajului. Cu toate acestea, trebuie să existe o cheie unică între oricare doi utilizatori. Astfel, odată cu creșterea numărului de utilizatori devine extrem de dificil să fie generate, distribuite și ținute în evidență aceste chei secrete. [1]

Un criptosistem cu chei publice folosește o pereche de chei: o cheie privată, cunoscută doar de către cel care o deține și o cheie publică, cunoscută de oricine dorește să comunice cu respectiva persoană. Pentru ca mesajul trimis să fie confidențial acesta este criptat cu cheia publică a receptorului, iar acest mesaj poate fi acum decriptat doar de receptor cu cheia privată asociată cheii publice cu care a fost criptat mesajul, cheie privată pe care o cunoaște doar receptorul. În ceea ce privește autentificarea, un mesaj poate fi criptat cu cheia privată a emițătorului, pe care îl vom referi ca A. Acest mesaj poate fi acum decriptat de oricine folosește cheia publică a lui A. Dacă aceasta duce la obținerea mesajului propriu-zis, atunci este evident că mesajul a fost criptat de cheia privată a lui A, astfel că doar A ar fi putut să trimită mesajul.[1]

Crearea și verificare unei semnături digitale

O schemă simplă pentru crearea și verificarea unei semnături digitale este prezentată în figurile 1 și 2. O funcție de hash este aplicată peste mesaj, obținându-se un rezumat al mesajului de dimensiune fixă. Funcția de semnare folosește hash-ul mesajului și cheia privată a emițătorului pentru a genera semnătura digitală. O formă foarte simplă de semnătură digitală este obținută prin criptarea hash-ului mesajului cu cheia privată a emițătorului. Mesajul nu este criptat și poate fi citit de oricine. Cu toate acestea, semnătura asigură autenticitatea emițătorului (aceasta poate fi comparată cu un document emis de o autoritate pentru a fi citit de mai multe persoane, acest document conținând și o semnătură care să ateste autenticitatea mesajului). Pentru receptor, funcția inversă este aplicată, practic decriptarea, pentru a obține hash-ul mesajului. Mesajul primit în clar este trecut acum prin aceeași funcție de hash ca mesajul original. Acum cele două hash-uri sunt comparate (cel obținut după decriptare cu cheia publică cu cel obținut după

aplicarea funcției de hash pe mesajul primit), iar dacă acestea sunt identice înseamnă că mesajul este într-adevăr trimis emițătorul legitim și mai înseamnă că acest mesaj nu a fost modificat. [1]

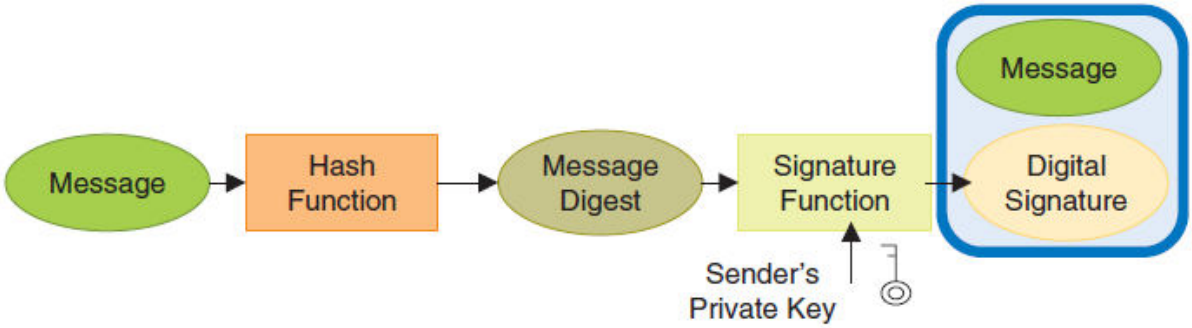

Fig. 1 Crearea unei semnături digitale [1]

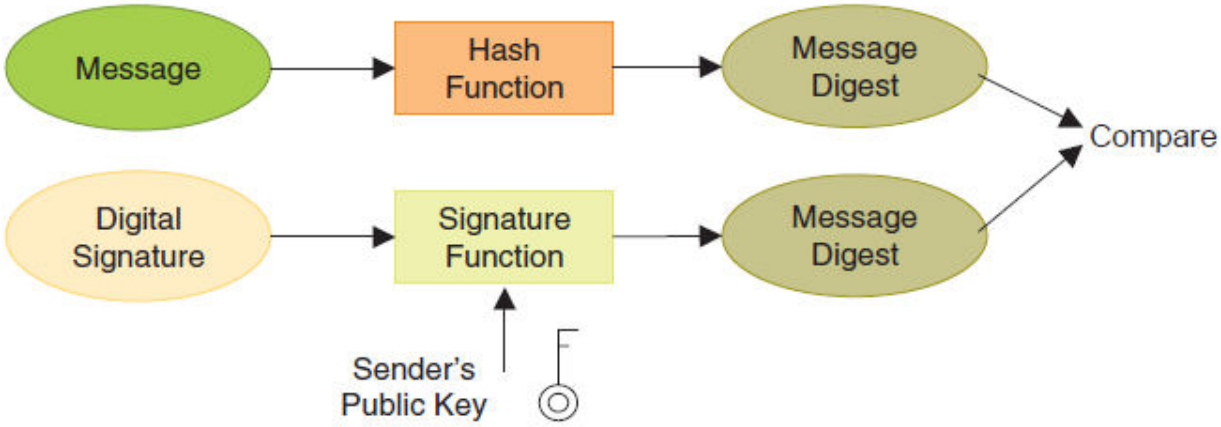

Fig. 2 Verificarea unei semnături digitale [1]

Importanța standardelor

În industria telecomunicațiilor, este acceptat de mult timp că standardele decid caracteristicile fizice, electrice și procedurale ale echipamentelor folosite pentru comunicare. În trecut, această viziune nu a fost îmbrățișată de industria calculatoarelor. În timp ce furnizorii de echipamente de comunicații recunosc că echipamentul lor va comunica în general cu echipamente provenite de la alți furnizori, producătorii de calculatoare, au încercat în mod tradițional să-și monopolizeze clienții. Înmulțirea calculatoarelor și procesarea distribuită au făcut ca o astfel de poziție să fie de neconceput. Calculatoarele provenite de la producători diferiți trebuie să comunice între ele și, odată cu evoluția continuă a standardelor protocoalelor de comunicare, cumpărătorii nu vor mai accepta dezvoltarea de soft cu scopul conversiei unui protocol.[2]

Există un număr de avantaje și dezavantaje în procesul de creare al standardelor. Principalele avantaje sunt următoarele [2]:

- un standard asigură faptul că va exista o piață de desfacere largă pentru un echipament sau un produs software. Aceasta încurajează producția în masă și, în unele cazuri, folosirea tehnicilor de integrare pe scară largă – *large-scale-integration* – (LSI) sau pe scară foarte largă – *very-large-scale-integration* – (VLSI), ceea ce rezultă în costuri scăzute.
- un standard permite produselor provenite de la producători diferiți să comunice, oferind cumpărătorului o mai mare libertate în alegerea și folosirea unui echipament.

Principalele dezavantaje ale standardelor sunt [2]:

- un standard tinde să înghețe tehnologia. Până când un standard este dezvoltat, revizuit și analizat astfel încât să se ajungă la un acord comun, după care este promulgat, există posibilitatea să se descopere tehnici mult mai eficiente decât cea standardizată.
- există mai multe standarde pentru aceeași tehnologie. Acesta nu este un dezavantaj al standardului în sine, ci al modului în care lucrurile funcționează în mod curent. Din fericire, organizațiile de standardizare cooperează destul de aproape. Cu toate acestea, încă sunt multe zone unde există conflicte între standarde.

ETSI – prezentare generală

Institutul European pentru Standarde în Telecomunicații - *European Telecommunications Standards Insititute* - (ETSI) este o organizație independentă, nonprofit, de standardizare din industria telecomunicațiilor (producători de echipamente și operatori de rețea) din Europa, cu sediul în Sophia-Antipolis, Franța, cu proiecție la nivel mondial. ETSI produce standarde globale aplicabile tehnologiilor informației și comunicațiilor (TIC), inclusiv tehnologiilor fixe, mobile, radio, convergente, boradcast și tehnologiilor internet [4].

ETSI a fost creată de CEPT în 1988 și este recunoscută oficial de către Comisia Europeană și secretariatul EFTA. Înființată în Sophia Antipolis (Franța), ETSI este responsabilă în mod oficial pentru standardizarea tehnologiilor informației și comunicațiilor (TIC) în Europa [5].

ETSI publică anual între 2.000 și 2.500 de standarde. De la înființarea sa în 1988, a produs peste 30.000. Acestea includ standarde care permit tehnologii globale foarte importante, cum ar fi sistemul de telefonie mobilă GSM, 3G, 4G, DECT, TETRA și sistemul de telecomunicații mobile TETRA, precum și cerințe privind dispozitivele de distanță scurtă, incluzând radio LPD, carduri inteligente și multe altele.

Comisiile tehnice competente ale ETSI și grupurile de specificații din industrie (ISG) includ SmartM2M (pentru comunicațiile între mașini), sisteme inteligente de transport, virtualizarea funcțiilor de rețea, securitatea informatică, semnături electronice și infrastructuri etc. ETSI a inspirat crearea, și este un partener, 3GPP și oneM2M. Toate comisiile tehnice, grupurile de lucru și industria de specificații sunt accesibile prin portalul ETSI.

Grupurile tehnologice ETSI oferă o imagine de ansamblu simplă și ușor de înțeles a activităților ETSI în domeniul standardizării TIC. Fiecare cluster tehnologic reprezintă o componentă majoră a unei arhitecturi TIC la nivel mondial și acoperă activitatea unui număr de comisii tehnice și a grupurilor de lucru ale ETSI, care au un domeniu și o viziune tehnologică comună. Activitatea unui singur Comitet Tehnic poate fi reprezentată în mai multe clustere. Clusterele facilitează identificarea cu ușurință a unei zone de interes bazată pe relevanța întreprinderii sau pe domeniul aplicației, mai degrabă decât pe domenii tehnice specifice de lucru.

În 2013, bugetul ETSI a depășit 23 de milioane de euro, contribuțiile provenind de la membri, activități comerciale precum vânzarea de documente, testele plug-in și găzduirea forumurilor [5], munca în contracte și finanțarea partenerilor [6].

ETSI este o organizație-partener fondator al inițiativei Global Standards Collaboration.

Protocolul ETSI TS 119 442 de validare a semnăturilor electronice

- **ETSI TS 119 442** definește un protocol care permite unui client să solicite validarea sau validarea și augmentarea semnăturilor digitale la un server de la distanță și permite serverului să returneze rezultatul validării clientului solicitant și, la cerere, semnătura să fie sporită în consecință. [7]
- **ETSI TS 119 442** prezintă două implementări pentru protocolul menționat anterior, una de tip XML, iar cealaltă de tip JSON. [7]
- Acest protocol permite solicitarea validării (și optional augmentarea) și returnează rezultatul validării (și semnătură sporită atunci când este cazul) pentru următoarele tipuri de semnături digitale [7]:
    - semnături CMS
    - semnături PDF
    - semnături XML
    - semnături CadES în conformitate cu ETSI EN 319 122, ETSI TS 101 733 sau ETSI TS 103 173
    - semnături PadES în conformitate cu ETSI EN 319 142, ETSI TS 102 778 sau ETSI TS 103 172
    - semnături XadES în conformitate cu ETSI EN 319 132, ETSI TS 101 903 sau ETSI TS 103 171
- Acest protocol suportă anveloparea de semnături, semnături anvelopate sau izolate.
- Acest protocol acceptă obiecte semnate în sine, hash-ul acestora sau rezultatul trecerii obiectelor print-o secvență de transformări (ultimul numai pentru documente XML și semnături XML sau XadES). [7]
- Acest protocol suportă un management asincron al cererilor și răspunsurilor.[7]

Abordarea tehnică pentru ETSI TS 119 442

- Ambele implementări ale protocolului au ca punct de plecare protocoalele specificate de „OASIS Digital Signature Service eXtended Technical Committee” (DSS-X TC) [7].
- Ambele implementări ale protocolului definit în ETSI TS 119 442 sunt profiluri ale documentului de bază 2.0 al OASIS DSS-X TC, care este în curs de producție OASIS.
- ETSI ESI și OASIS DSS-X TC au semnat o înțelegere care să permită schimbul reciproc de informații și participarea reprezentaților unei părți la ședințele celeilalte părți.
- Pentru fiecare componentă a protocolului, ETSI TS 119 442 definește: specificația sa semantică, o specificație XML completă și o specificație JSON completă.
    - **specificația semnatică**: include, printre altele, funcționalitatea componentei, a componentelor acesteia (dacă există) sau semantica valorii sale, dacă este cazul. Această specificație semantică este independentă de implementarea protocolului (XML sau JSON).

- **specificația XML completă**:
  - o schemă de definiție XML a componentei dacă această componentă nu este luată din specificațiile OASIS DSS-X, SAU
  - o referință la schema de definiție XML a componentei dacă această componentă este definită într-o sepcificație OASIS DSS-X și este profilată în continuare aici.
  - specificarea modelului de procesare pentru server dacă ce trebuie procesat nu este luat din specificațiile OASIS DSS-X SAU dacă această componentă ce trebuie procesată este luată din specificațiile OASIS DSS-X, dar este profilată în continuare aici.
  - documentul este tacit dacă modelul de procesare este egal cu cel specificat în documentația OASIS DSS-X corespunzătoare.
- **specificația JSON completă**:
  - schemă de definiție JSON a componentei dacă această componentă nu este luată din specificațiile OASIS DSS-X, SAU
  - referință la schema de definiție JSON a componentei dacă această componentă este definită într-o sepcificație OASIS DSS-X și este profilată în continuare aici.
  - specificarea modelului de procesare pentru server dacă ce trebuie procesat nu este luat din specificațiile OASIS DSS-X SAU dacă această componentă ce trebuie procesată este luată din specificațiile OASIS DSS-X, dar este profilată în continuare aici.
  - documentul este tacit dacă modelul de procesare este egal cu cel specificat în documentația OASIS DSS-X corespunzătoare.

Prezentarea generală a mesajului de solicitare a validării: mesajul de cerere, documentele și semnăturile

Componentele cererii:

- o componentă ce conține semnătura ce trebuie validată.
- o componentă (sau mai multe) ce conține documentul/ele sau o reprezentare a acestora, ex. hash-ul acestora sau rezultatul unor transformări aplicate acestor documente.
- opțional componente pentru caracteristici adiționale.

Componente pentru semnătură și documente semnate:

- permite orice tip de plasare relativă a semnăturii și a documentelor semnate, și anume: anveloparea semnăturii, semnătura anvelopată, semnătura izolată și orice combinație a acestora (combinație care este posibilă în semnături XML și XAdES).
- plasarea specifică a semnăturii și a documentelor semnate în mesajul solicitant depinde de poziția lor relativă:
  - semnăturile învelite în cadrul unui document vor fi plasate în componenta **DocumentWithSignature**.
  - semnăturile care nu sunt înfășurate vor fi plasate în componenta **Signature**.

- documentele detașate și reprezentările documentelor semnate (hash-ul acestorea sau transformarea) vor fi plasate în componenta **Document**.
- documentele învelite în semnăturile de înfășurare vor fi plasate în componenta **Signature**.

Hint-uri pentru componentele opționale:

- Componentă pentru solicitarea utilizării unui anumit moment de timp ca timp de validare.
- Componentă pentru solicitarea returnării timpului de validare utilizat.
- Componentă pentru solicitarea returnării identității semnatarului.
- Componentă pentru solicitarea utilizării unei anumite politici de validare a semnăturii. Această componentă permite, de asemenea, specificarea locului unde poate fi accesată politica de validare a semnăturii.
- Componentă pentru solicitarea returnării unui raport detaliat de validare conform cu ETSI TS 119 102-2 (a căror producție se încadrează în domeniul de aplicare al STF 524).
- În cazul semnăturilor XML și XAdES, se solicită validarea individuală a semnăturii: elemente manifest.
- Componentă pentru identificarea solicitării depuse.
- Componentă pentru gestionarea procesării asincrone: componentă pentru identificarea unei solicitări ca o cerere ulterioară după o cerere inițială sau după o altă solicitare ulterioară.

Prezentarea generală pentru răspunsul de validare: mesajul de răspuns

Componentele răspunsului:

- Componentă pentru notificarea rezultatului validării.
- Componentă care indică faptul că răspunsul a fost construit folosind protocolul specificat în ETSI TS 119 442.
- Componente opționale pentru caracteristici suplimentare

Componentă pentru notificarea rezultatului validării:

- O componentă majoră ce specifică dacă procesul de validare a fost corect efectuat sau nu.
- O componentă minoră opțională care rezumă rezultatul validării. În cazul în care cererea a inclus componenta care solicită returnarea unui raport de validare detaliat, această componentă nu va fi prezentă (toate detaliile vor fi prezente în raportul menționat mai sus).

Hint-uri pentru componentele opționale:

- Componentă ce returnează timpul de validare utilizat.
- Componentă pentru returnarea identității semnatarului.
- Componentă pentru specificarea politicii de semnătură față de care semnătura a fost validată.

- Componentă pentru specificarea politicilor de semnătură față de care serverul poate valida semnături. Această componentă poate fi inclusă într-un răspuns în cazul în care serverul nu a putut valida o semnătură față de o politică de validare cerută.
- Componentă pentru returnarea unui raport de validare detaliat conform cu ETSI TS 119 102-2.
- Componentă pentru returnarea unui raport de validare detaliat semnat conform cu ETSI TS 119 102-2.
- În cazul semnăturilor XML și XAdES, o componentă pentru returnarea rezultatului din ds: elemente manifest.
- Componentă pentru indicarea faptului că validarea semnăturii nu a fost încă finalizată. Aceasta este una dintre componentele folosite pentru gestionarea procesării asincrone.
- Componentă pentru corelarea cererilor ulterioare răspunsului inițial. Acest element trebuie să conțină un identificator pe care clientul îl va include în solicitări ulterioare astfel încât acestea să poată fi corelate cu cererea inițială. Aceasta este a doua componentă utilizată pentru gestionarea procesării asincrone.

Prezentarea generală a cererii de validare și augmentarea semnăturii

Componentele cererii:

- aceleași componente (cele obligatorii și opționale) ca cele pentru mesajul de cerere a validării semnăturii.
- o componentă pentru a cere, în plus, augmentarea semnăturii ce urmează să fie validată.

Componenta de cerere a augmentării semnăturii ce urmează să fie validată:

- trebuie să conțină nivelul tehnic la care trebuie să fie „sporită” semnătura ce urmează să fie validată.
- ETSI TS 119 442 definește un set de URI-uri, fiecare identificând diferite nivele specificate în documentația AdES generată de ETSI (ETSI TSs și ETSI Ens).

Prezentarea generală a mesajului de răspuns ce conține rezultatul validării și semnătura augmentată

Componentele răspunsului:

- aceleași componente (cele obligatorii și opționale) ca cele pentru mesajul de răspuns la o cerere de validare a semnăturii.
- o componentă folosită pentru returnarea semnăturii augmentate.

Componenta folosită pentru returnarea semnăturii augmentate poate să conțină ori:

- semnătura „sporită” dacă nu este înfășurată cu un document semnat.
- documentul cu semnătura augmentată, dacă semnătura este înfășurată în acest document

TS 119 102-2 RAPORT DE VALIDARE A SEMNĂTURII

Raportul de validare a semnăturilor digitale AdES conține [8]:

- o structură generală
- o implementare XML a structurii generale
- se aliniază cu cerințele specificate în EN 319 102 partea 1

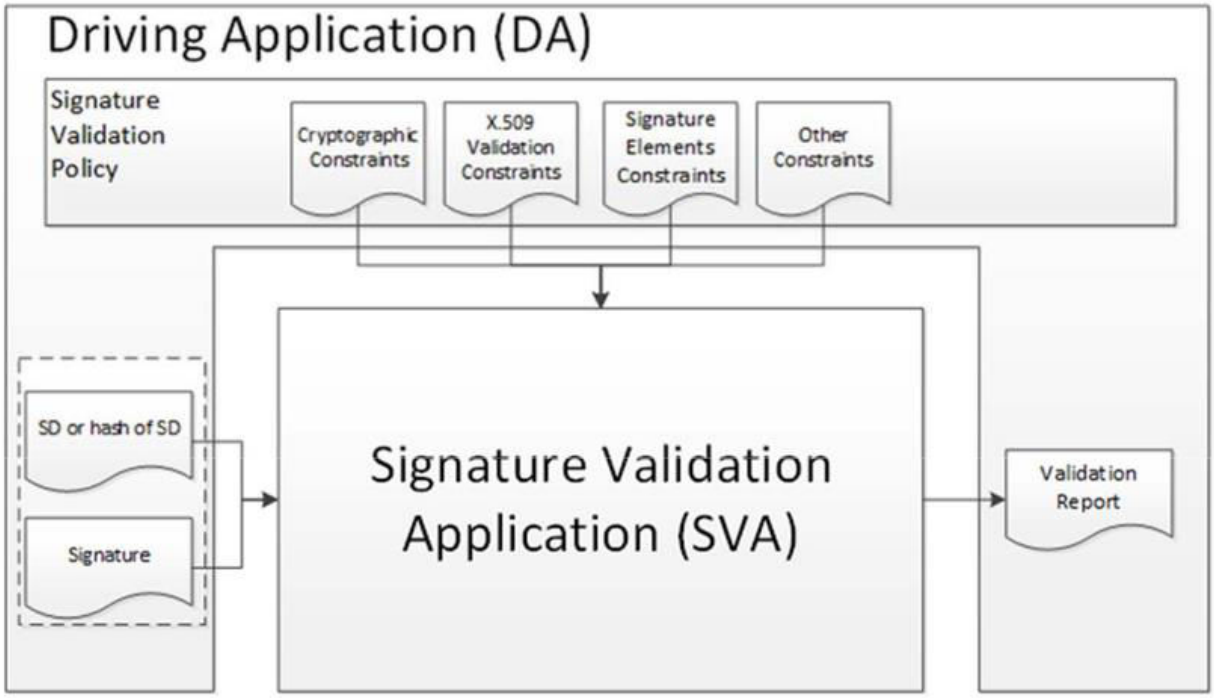

Fig. 3 Model conceptual de validare a semnăturii ETSI EN 119 102-1

Cerințe din 102-1 [8]:

- 5.1.1: SVA trebuie să furnizeze o indicație de stare și raportul de validare care oferă detaliile tehnice specifice fiecărei constrângeri aplicate, raport ce poate fi relevant pentru DA în interpretarea rezultatelor.
- 5.1.3: specifică minimul de cerințe pentru un astfel de raport:
  - indicație de stare;
  - politica sau setul de constrângeri față de care a fost realizată validarea;
  - data și timpul la care a fost determinat status-ul validării;
  - datele de validare utilizare;
  - date adiționale;

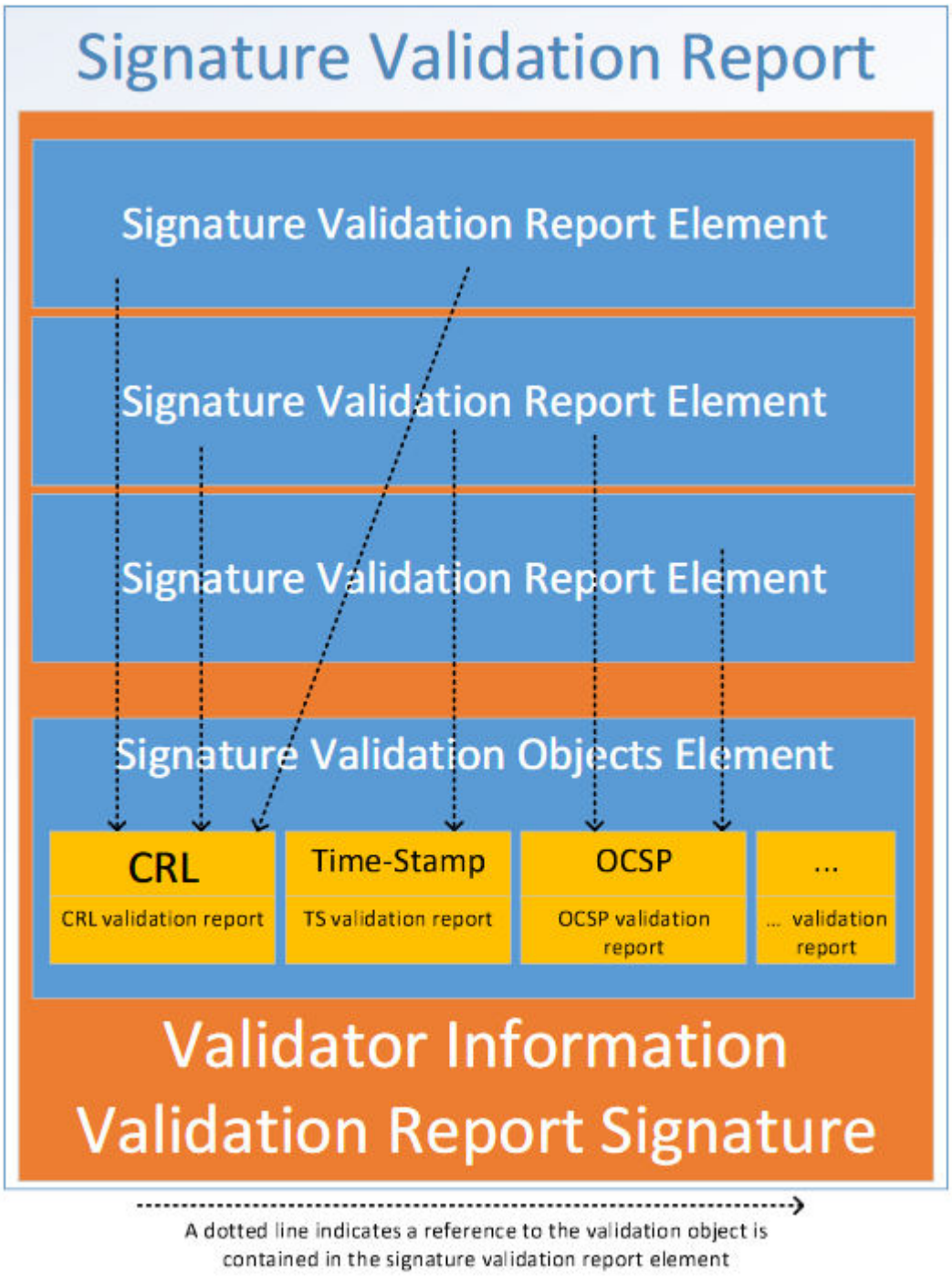

Fig. 4 Structura raportului de validare a semnăturii [11]

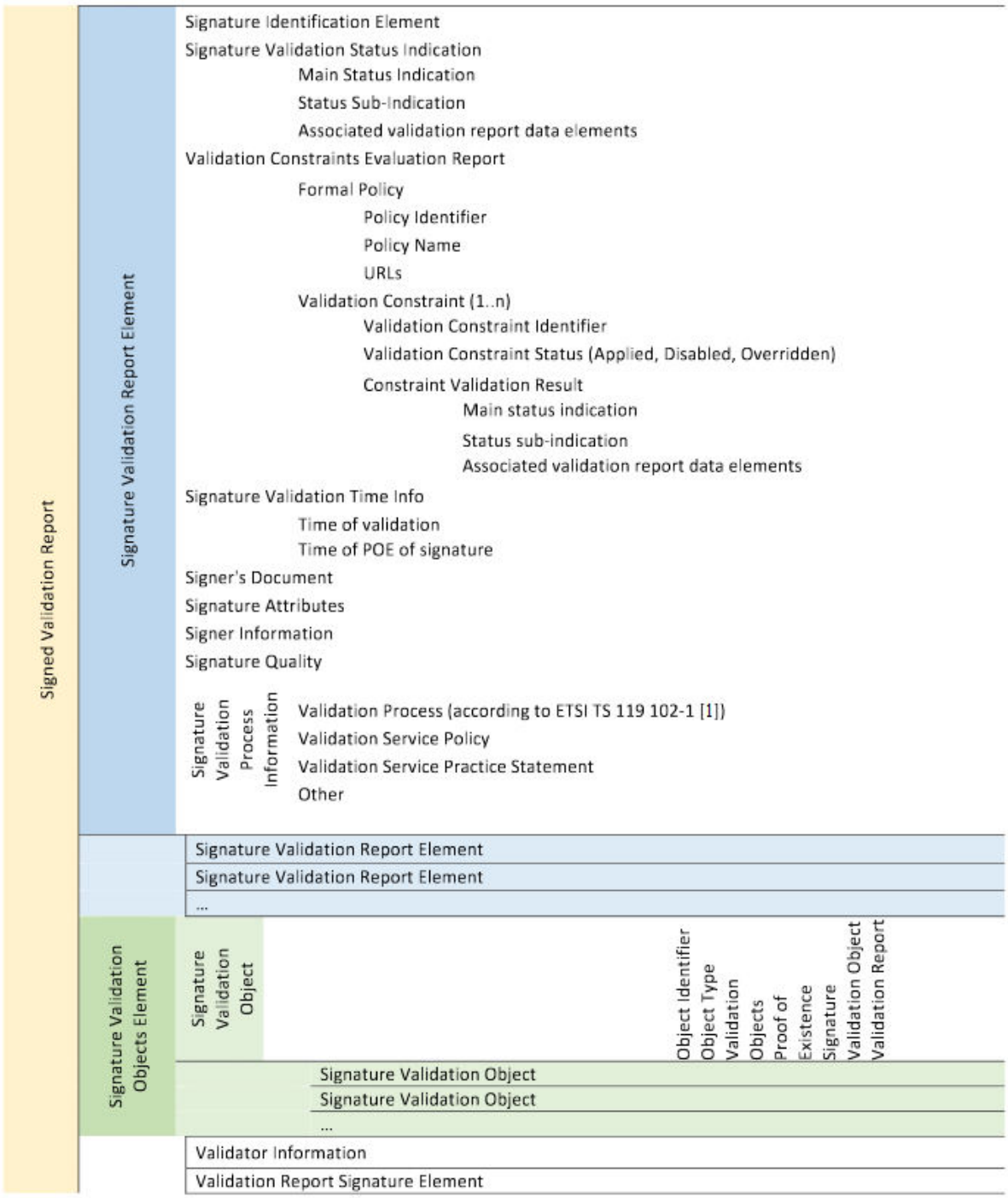

Fig. 5 Structura raportului de validare și elementele componente[11]

Concluzii și direcții de cercetare

Beneficiile principale obținute prin introducerea proceselor digitale de semnare sunt reducerea costurilor și automatizarea completă a fluxului de lucru cu documente, incluzând aici etapele de autorizare și de validare.

În esență, semnăturile digitale permit înlocuirea procesului de aprobare pe hârtie, proces lent și scump, cu un sistem complet digital, mai rapid, mai ieftin și mai sigur.

O semnătură digitală este o schemă matematică pentru verificarea autenticității mesajelor sau a documentelor digitale. O semnătură digitală validă asigură destinatarul că mesajul a fost creat de un expeditor cunoscut **autentificare**, că expeditorul nu poate nega că a trimis mesajul **non-repudiere** și că mesajul nu a fost modificat în tranzit **integritate**.

În continuare se dorește studierea amănunțită a [10] și [11].

Se vor studia diferite tipuri de implementări și tehnologii specifice serviciilor software, după care se vor stabili principalele direcții de implementare ale serviciului de validare a semnăturilor digitale în conformitate cu standardele ETSI.

Bibliografie

1. S.R. Subramanya, Digital signatures. IEEE Potentials. April 2006.
2. William Stallings.
   Cryptography and Network Security Principles and Practices, Fourth Edition. Prentice Hall. November 16, 2005.
3. ETSI (European Telecommunications Standards Institute). Gartner.Retrieved 27 September 2018. https://www.gartner.com/it-glossary/etsi-european-telecommunications-standards-institute
4. ETSI. https://en.wikipedia.org/wiki/ETSI
5. What we do. ETSI. Retrieved 27 September 2018. https://www.etsi.org/about
6. ETSI Annual Report. ETSI. Retrieved 1 February 2014. https://www.etsi.org/media-library/work-programme-and-annual-reports
7. ETSI TC ESI WORK ON E-SIGNATURES AND E-SEALS REMOTE VALIDATION PROTOCOL (ETSI TS 119 442). Juan Carlos Cruellas.
8. TS 119 102-2 – SIGNATURE VALIDATION REPORT. An Introduction. Peter Lipp. 10 Ianuarie 2018
9. ETSI Documents: http://www.etsi.org/standards-search
10. ETSI TS 119 102-2
    https://www.etsi.org/deliver/etsi_ts/119100_119199/11910202/01.01.01_60/ts_11910202v010101p.pdf?fbclid=IwAR2IRIxIhsa2Nv2bU4Q-F7RrzgU7Vkj0CGlPb1B4FtZ5YLU2Mld3h-_GPK8
11. ETSI TS 119 441
    https://www.etsi.org/deliver/etsi_ts/119400_119499/119441/01.01.01_60/ts_119441v010101p.pdf?fbclid=IwAR2IRIxIhsa2Nv2bU4Q-F7RrzgU7Vkj0CGlPb1B4FtZ5YLU2Mld3h-_GPK8